REMARKS

Claims 1-32 are pending.

The Office Action mailed July 13, 2005 rejected claims 1, 5-7, 9, 13-15, 17-23, 25-26, 28-29, and 31-32 under 35 U.S.C. § 103(a) as obvious over *Ji et al.* (U.S. 5,623,600) in view of *Xu* (U.S. Patent Application Publication No. 2002/0032766) and further in view of *Scott et al.* (U.S. 6,385,747), and claims 2-4, 8, 10-12, 16, 24, 27, and 30 under 35 U.S.C. § 103(a) as obvious over *Ji et al.* in view of *Xu* and *Scott et al.* and further in view of *Wells* (U.S. 6,338,141).

Applicants respectfully traverse the rejections under 35 U.S.C. § 103, in that none of *Ji et al., Xu, Scott et al.,* nor *Wells*, singly or in combination, discloses the claimed features.

For example, independent claims 1, 8, 9, and 16 each include the feature "**distributing a common copy of the flow** to each of the scanning computer systems in parallel." Independent claims 17, 18, and 19 each recite "**duplicating the flow** to produce a plurality of **common copies** of the flow." Independent claims 20 and 21 each recite "receiving **respective common copies of a flow of content** from the front-end processor in parallel." Independent claims 22, 25, and 28 each include the feature "receiving an alarm ... when **a common flow** of content **scanned by the scanning computer systems in parallel** contains malicious code, said common flow including at least one of a hypertext markup file and a transferred file."

Claim 1 clearly recites, "a **plurality of scanning computer systems** configured for scanning content for malicious code and generating an alarm when the content contains malicious code; and a front-end processor, coupled to the scanning computer systems, configured for **receiving a flow of content** from an external network and **distributing a common copy of the flow to each of the scanning computer systems in parallel for scanning**." Regarding claims 1 and 9, the Office Action (p. 4) correctly acknowledges, "Ji fails to teach distributing a common copy of the flow to each of the scanning computer systems in

parallel for scanning." The Office Action dated May 19, 2004 also correctly acknowledged this deficiency, and applied *Shanklin et al.* (U.S. 6,578,147) for a supposed teaching of "parallel sensors" (Office Action dated May 19, 2004, page 3, line 20 - page 4, line 13). The previous Office Action, having dropped its application of *Shanklin et al.*, apparently in response to persuasive arguments by Applicants, asserted instead, "the examiner asserts that the use of multiple virus scanning devices scanning a common copy of the flow in parallel is **well known in the art**." (Office Action dated January 27, 2005, p. 3, lines 3-4) The Examiner had apparently tried, but failed to produce evidence to support the assertion regarding this feature, and at that time relied solely on the "well known in the art" assertion to reject the claims. The present Office Action (p. 4) states:

> However, Xu discloses a plurality of scanning computer systems and distributing a common copy of the flow to each of the scanning computer systems for scanning, Xu, page 18, paragraphs 228 (Xu).
>
> It would have been obvious to one of ordinary skill in the art to modify Ji's scanning system to incorporate a plurality of virus scanning systems of Xu for scanning a common copy of the flow because different scanners with different capabilities are used as a "safety net" to improve the chances of detecting a virus, Xu, page 18, paragraphs 228 (Xu).
>
> It is noted that the combination of Ji and Xu fails to disclose (as Applicant persuasively argued) distributing a common copy of the flow to each of the scanning computer systems in parallel for scanning.
>
> However, Scott teaches a technique for broadcasting (i.e. distributing) the same test inputs (common copy of the flow), in parallel, used in testing (scanning) to each of the replicated components of an electronic device under test (Scott, abstract).
>
> Therefore, it would have been further obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Scott's parallel scanning systems within the system of Ji and Xu as combined above, in order to speed up the scanning process as suggested by Scott, col. 2, lines 63-67.

However, in explanation of the problems that it is directed to solving, *Xu* states, at ¶¶ 88-89:

[0088] Embodiments of the present invention provide capabilities that are not and cannot be supported by the known art technologies. Those technologies rely upon network traffic passing through a rigid sequence of systems. Embodiments of the present invention eliminate that constraint. As shown in FIG. 4, disparate users 21-23 have access to numerous applications via network 30 and system 400. In addition to network applications such as firewall 60, VPN 50, and virus wall appliance 55, the clients can access application servers 71-74 and other applications such as voiceover-IP (VoIP) system 441 and load balancing server 442. Router 45 is a conventional IP router.

[0089] Embodiments of the present invention use packet direction, packet distribution, and an advanced **packet sequencing feature to direct packets through a customized sequence of application systems that is defined, on demand, by the customer.** Embodiments of the present invention can maintain each customized sequence as a series of MAC/IP addresses and communication interfaces. The customer can access the sequence via a service IP address and a subordinate service port. Embodiments of the present invention also remove access control responsibilities from the firewalls that they direct and enable dynamic access control management by the subscriber or end-user.

Further, *Xu* states, at page 18, ¶ 228:

In FIG. 23, the ISP network 2390 includes a packeting engine 2300 between clients 2321-2323 and the network service providers 2381-2383 coupled to the Internet 2385. The packeting engine 2300 directs the client packets through **a series of appliances**, including an intrusion detection system 2351 **one or more virus scanning devices 2352-2353**, and one or more of firewalls 2361-2363. Since companies that create virus scanning software differ in their capabilities to detect viruses and to issue timely virus signature updates, multiple virus scanning devices may be used as a "safety net" to improve the chances of detecting a virus. In previous examples of the invention, embodiments of a packeting engine used a service IP address to direct packets and disregarded the client's address. To perform its role in the ISP solution, an embodiment of a packeting engine 2300 can be configured to do just the opposite, i.e., use the client's IP address as the service IP address. Therefore, the **sequence of appliances is determined from the service IP address**, which is actually the client address that was assigned by the ISP 2390.

Thus, *Xu* specifically requires that processing of packets be performed by predefined, specific **sequences** of appliances such as the virus scanning devices 2352 and 2353. Moreover, the **customized sequence of application systems is defined, on demand, by the customer**. The cited portion of *Xu* refers to the ordering of a processing sequence as being determined by a

service IP address, and thus *Xu* has nothing to do with "**distributing a common copy of the flow** to each of the scanning computer systems **in parallel**" as recited by claims 1, 8, 9, and 16 but instead teaches away from such parallel operations, as such parallel operations would be technically unfeasible in such an "on demand" sequencing environment.

Scott et al. (per Abstract, emphasis added) states:

> A technique is provided for use in **testing** replicated components (e.g., **identical circuit components**) of an electronic device for defects. In one aspect of this testing technique, the **same test inputs** may be broadcast, in parallel, **from a single test interface** to each of the replicated components of the electronic device under test. Respective test outputs generated by the replicated components in response to the test inputs may be supplied to a comparator, comprised in the electronic device, that compares the respective test outputs to each other and **generates a fault signal if corresponding test outputs are not identical**. This fault signal may be supplied to an **external test interface pin of the single test interface**, and its assertion may indicate that one or more of the replicated components may be defective. The respective test outputs may be multiplexed to permit output via an external interface of respective test outputs from a selected component. These respective test outputs may be compared to expected values therefor whereby to determine presence and/or nature of defects in the replicated components.

Thus, *Scott et al.* is directed to broadcasting test inputs in parallel to **identical circuit components** for **testing the components**, and a fault signal is to be generated if the test outputs are not **identical**. This type of **component testing** described by *Scott et al.* has nothing to do with any "**plurality of scanning computer systems configured for scanning content for malicious code** and generating an alarm when the content contains malicious code" as recited by claim 1, nor does it have anything to do with any type of "**customized sequence of application systems**" that is **"defined, on demand, by the customer,"** as is disclosed by *Xu*. In fact, the parallel testing of *Scott et al.* teaches away from the customized sequencing of *Xu*. Moreover, as stated by the Office Action regarding the advantages of *Xu*, "**different scanners with different capabilities** are used as a 'safety net' to improve the chances of detecting a virus, Xu, page 18, paragraphs 228 (Xu)." It is improper to combine references where the references

teach away from their combination. *In re Grasselli*, 713 F.2d 731, 218 USPQ 769 (Fed. Cir. 1983). A prior art reference must be considered in its entirety including portions that would lead away from the claimed invention. *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984).

The addition of *Wells*, applied for supposedly teaching using a collection of relational data to detect computer viruses (Office Action, pp. 14, 15, 16, 17), fails to cure the deficiencies of *Ji et al.*, *Xu*, and *Scott et al.* as discussed previously. Thus, the rejections of independent claims 1, 8, 9, 16, 17, 18, 19, 20, 21, 22, 25, and 28, should be withdrawn.

Dependent claims 2-7, 10-15, 23-24, 26-27, and 29-32 are allowable for at least the same reasons as their respective independent claims, and are separately patentable on their own merits. For example, dependent claim 5, which depends from claim 1, recites, "wherein each of the scanning computer systems is configured to execute respective anti-virus scanning software having different, corresponding coverage of malicious code." The Office Action (p. 5) relies on *Xu* as disclosing this feature, in combination with *Ji et al. and Scott et al.* As discussed previously, *Scott et al.* teaches away from this feature, and thus the rejection should be withdrawn.

Moreover, Applicants respectfully submit that "a need for a malicious code detection system and methodology with the good anti-viral coverage of multiple anti-virus scanners but characterized by the low latency commensurate with that of a single anti-virus scanner" was recognized by the Applicants (specification, ¶ 9), and was solved by the present claimed invention (*See*, e.g., specification, ¶ 10). It is well settled that the problem addressed and solved by a claimed invention must be given consideration in resolving the ultimate legal conclusion of obviousness under 35 U.S.C. § 103. *North American Vaccine, Inc. v. American Cyanamid Co.*, 7 F.3d 1571, 28 USPQ 1333 (Fed. Cir. 1993); *In re Dillon*, 919 F.2d 688, 16 USPQ2d 1897 (Fed.

Cir. 1990); *Northern Telecom, Inc. v. Datapoint Corp.*, 908 F.2d 931, 15 USPQ 1321 (Fed. Cir. 1990); *Jones v. Hardy*, 727 F.2d 1524, 220 USPQ 1021 (Fed. Cir. 1984). The Office Action has failed in this regard as well, instead applying impermissible hindsight to assert that features recited by the claims are taught by untenable combinations of the applied references. Thus, the rejections of all pending claims should be withdrawn.

Therefore, the present application overcomes the objections and rejections of record and is in condition for allowance. Favorable consideration is respectfully requested. If any unresolved issues remain, it is respectfully requested that the Examiner telephone the undersigned attorney at (703) 425-8508 so that such issues may be resolved as expeditiously as possible.

Respectfully Submitted,

DITTHAVONG & CARLSON, P.C.

10/13/05
Date

Reg. No. 44,658

Margo Livesay, Ph.D.
Attorney/Agent for Applicant(s)
Reg. No. 41,946

10507 Braddock Road
Suite A
Fairfax, VA 22032
Tel. (703) 425-8508
Fax. (703) 425-8518